PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04Q 7/38 — A1

(11) International Publication Number: **WO 00/24218**

(43) International Publication Date: 27 April 2000 (27.04.00)

(21) International Application Number: PCT/SE99/01786

(22) International Filing Date: 6 October 1999 (06.10.99)

(30) Priority Data:
9803569–4 19 October 1998 (19.10.98) SE

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S–126 25 Stockholm (SE).

(72) Inventor: HALLENSTÅL, Magnus; Täbyvägen 220, S–187 50 Täby (SE).

(74) Agents: SANDSTRÖM, Staffan et al.; Bergenstråhle & Lindvall AB, P.O. Box 17704, S–118 93 Stockholm (SE).

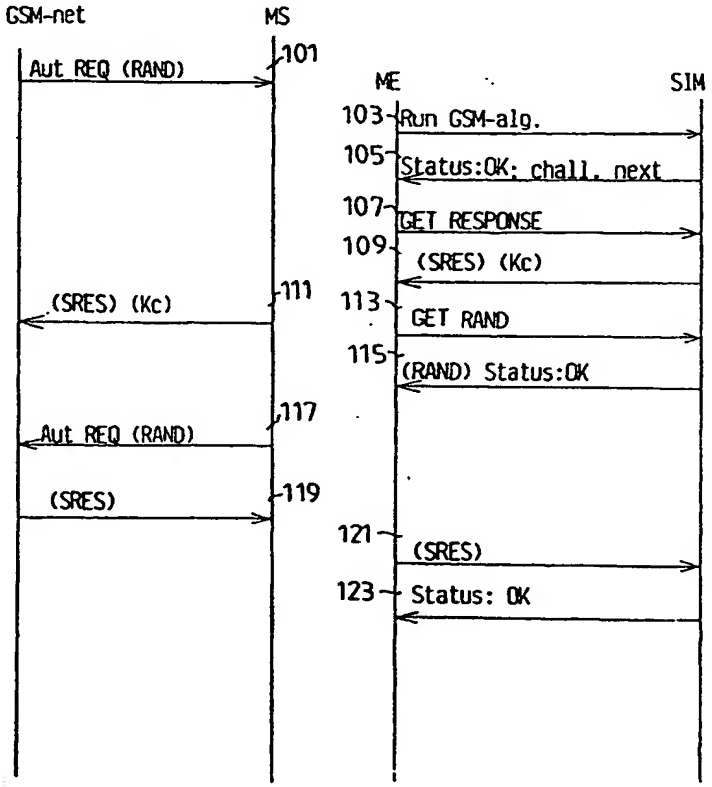
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD AND A SYSTEM FOR AUTHENTICATION

(57) Abstract

In a method and a system for increasing the security in a system comprising and communicating with a removable memory card, such as a SIM card or smart card a new function is added in the existing SIM card so that the SIM–card will challenge the system. Thus, the SIM–card will issue a random number towards the network and the network then has to respond with a correct result. If not the SIM–card will be automatically switched off. The use of the method and the system will reduce the risque for someone to find out the correct code of the removable memory card by means of a massive test. The method can also be employed in other systems where the system communicates with an electronic device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

A METHOD AND A SYSTEM FOR AUTHENTICATION

TECHNICAL FIELD

The present invention relates to a method and a system for increasing the security in a system comprising and communicating with a removable memory card, such as a SIM card or a smart card.

BACKGROUND OF THE INVENTION AND PRIOR ART

In existing mobile telecommunication systems, for example the GSM (Global System for Mobile communication) system, SIM-cards (Subscriber Identity Module) are used for providing each user with a unique identity. Thus, the GSM system provides communication between a base station and one or several Mobile Stations (MS). Each Mobile Station (MS) comprises a Mobile Equipment (ME) for handling the communication between the Mobile Station (MS) and a SIM card for providing each Mobile Station with a unique identity.

The security aspects of GSM are described in the normative references GSM 02.09 (ETS 300 920): "Digital cellular telecommunications system; Security aspects" and GSM 03.20 (ETS 300 929): "Digital cellular telecommunications system; Security related network functions".

One important security aspect is the authentication of the subscriber identity to the network. Below the authentication and cipher key generation procedure according to the GSM standard is outlined:

First, the network sends a Random Number (RAND) to the Mobile Station (MS). The Mobile Equipment (ME) passes the random number to the SIM card. At the same time a command "RUN GSM ALGORITHM" is given to the SIM card as described in GSM 03.20 (ETS 300 929): "Digital cellular telecommunications system; Security related network functions". The SIM returns the values Signed RESponse calculated by a SIM (SRES) and Cryptographic key (Kc) to the mobile equipment. The ME sends SRES to the network. The network compares this value with the value of SRES which it calculates for itself. The comparison of these SRES values provides the authentication. The value Kc is used by the ME in

any future enciphered communications with the network until the next invocation of this mechanism.

The security provided by the GSM system has until now been sufficient. However, using modern technology it has become possible to crack the very secret unique key stored in each SIM card and also the secret algorithm used in the authentication process. The method used is to send a very large amount of test samples to the SIM card and then analyze the results returned by the SIM card. In this manner it has become possible to clone SIM cards.

SUMMARY

It is an object of the present invention to increase the security on SIM-cards, smart cards and similar devices, and in particular to increase the security for a GSM SIM-card and to avoid that the SIM card can be cracked.

This object is obtained by means of adding a new function in the existing SIM card so that the SIM-card will challenge the system. Thus, the SIM-card will issue a random number towards the network and the network then has to respond with a correct result. If not the SIM-card will be automatically switched off.

The use of such a new functionality on the SIM-card will significantly increase the security thereof. Thus, it will reduce the risque for someone to find out the correct code of the SIM card by means of a massive test.

The method can also be used in other systems than the GSM system, where it is imperative that the removable memory card should not be cracked. An example is when money are stored on a card ("electronic money") and where the amount can be refilled. Other application areas are also possible. Thus, it is possible to use the method as described herein in many kinds of electronic devices. Means for executing the method can be provided in integrated circuits, mobile telephones, modems, etc. An authentication unit for providing additional security can in this manner easily be provided in existing systems.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail by way of non-limiting examples and with reference to the accompanying drawings, in which:

- Fig. 1 is a flow chart illustrating different steps carried out when verifying the authenticity of a SIM-card located in a Mobile Station (MS) communicating with a network.
- Fig. 2 is a flow chart illustrating an alternative scheme according to a second embodiment.

DESCRIPTION OF PREFERRED EMBODIMENTS

In Fig. 1 a flow chart illustrating different steps carried out during authentication in a GSM system is shown. Thus, first a Mobile Station (MS) receives a random number from the GSM network, step 101. Thereupon, the Mobile Equipment (ME) of the MS issues a command "RUN GSM algorithm", as described above, step 103. The SIM card then returns a status condition indicating that the status is OK and that a challenge towards the system should be issued before the command "RUN GSM algorithm" can be issued again, step 105. This could for example be carried out by adding a new code as a response to the command "RUN GSM algorithm".

Next, the ME requests the response from the SIM card, step 107 and the SIM card returns the values Signed RESponse calculated by a SIM (SRES) and Cryptographic key (Kc) to the mobile equipment, step 109. The MS then returns the SRES and the Kc to the GSM network as an authentication of the SIM card as described above, step 111.

Next, the ME issues a request for a random number to the SIM card, step 113 as a response to the message in step 105, which indicated that a challenge should be transmitted to the GSM network. The SIM card then returns a random number and a status OK message, step 115. Thereupon, the MS issues a request towards the GSM network for authentication thereof by means of transmitting the random (RAND) number to the GSM network. The GSM network then has to respond to this request, preferably by

means of returning an SRES, which then can be verified by the SIM, see below. Thus, the GSM network responds with a SRES value to the MS, step 119.

The SRES received by the MS is the transmitted from the ME to the SIM card, step 121. The SIM card then verifies that the SRES value is the correct value and, if so, returns a status: OK message to the ME, step 123.

If the GSM system does not respond or the SRES returned by the GSM system is not the correct one, the ME will start over again with the authentication process of the GSM system, thus starting the procedure with step 113. The ME will continue to execute this process until the system replies with a correct answer, or until a certain, pre-set random numbers have been issued, without the system replying with a correct number. The SIM will indicate when no more challenges can be issued in the response indication in step 115.

If the system fails to reply with a correct number or code, the SIM card turns itself off, i.e. it does not respond to any requests sent to it.

In Fig. 2 a second embodiment for authenticating the GSM network is shown. Thus, first a Mobile Station (MS) receives a random number from the GSM network, step 201. Thereupon, the Mobile Equipment (ME) of the MS issues a command "RUN GSM-algorithm", step 203. The SIM card then returns a status condition indicating that the status is not OK and that a challenge towards the system should be issued, step 205. This could for example be carried out by adding a new code as a response to the command "RUN GSM algorithm".

Next, the Mobile Equipment issues a request for a random number to the SIM card, step 207. The SIM card returns a random number (RAND2) together with a status: OK message, step 209.

This random number is then transmitted towards the system by the mobile station, step 211. The GSM system then returns an SRES

value (SRES2), step 213. Next, the ME transmits the SRES value (SRES2) to the SIM card, step 215. The SIM card then compares this value with the value of SRES2 which it calculates for itself. The comparison of these SRES values provides the system authentication and the SIM returns an acknowledge message (status: OK) to the Mobile Equipment if the compared SRES2 values match, step 217.

If the GSM system does not respond or the SRES2 returned by the GSM system is not the correct one, the ME will start over again with the authentication process of the GSM system, thus starting the procedure with step 207. The ME will continue to execute this procedure, until the system replies with a correct answer, or until a certain, pre-set random numbers have been issued, without the system replying with a correct number. The SIM will indicate when no more challenges can be issued in the response indication in step 209.

If the system fails to reply with a correct number or code, the SIM card turns itself off, i.e. it does not respond to any requests sent to it.

As a response to the message in step 217 the ME issues the command RUN GSM algorithm towards the SIM card, step 219. The SIM card the responds with a status: OK message, step 221. Next, the ME issues a command GET RESPONSE towards the SIM card, step 223. The SIM card the responds with the SRES and the Kc as described above, step 225. The SRES and the Kc is then transmitted by the MS to the GSM system as authentication of the SIM card, step 227.

In a preferred embodiment the SIM card only challenges the system, i.e. sends a random number to the system, every N time, N being a positive integer > 1, that the system challenges the SIM card.

The method and system as described herein can also be employed in other kinds of systems than the systems described above. Thus, the method is possible to use in any system provided with

means for authenticating an electronic device connected to the system. The system will then comprise a first authentication unit which then communicates with a second authentication unit located in the electronic device using a method corresponding to the method described above.

The method and system as described herein provides a significantly increased security for different kinds of removable memory card, such as SIM cards, smart cards, and other kinds of systems where a mutual authentication process between an electronic device and the system is required for ensuring an acceptable security.

CLAIMS

1. A method of authentication in a system comprising and communicating with a removable memory card, **characterized by** the steps of:
- issuing a random number from the card,
- returning a number from the system to the card,
and that the card authenticates the system if the returned number is a correct number as verified by an algorithm stored on the card, which is fed with the same random number.

2. A method according to claim 1, **characterized in** that the card turns itself off if the returned number is incorrect.

3. A method according to claim 2, **characterized in** that the card only turns itself off if the system returns an incorrect number N consecutive times, N being a positive integer > 1.

4. A method according to any of claims 1 - 3, when the system is a cellular radio system, in particular a GSM system, and the removable memory card is a SIM card, **characterized in** that the authentication of the system is issued in conjunction with the authentication of the SIM card by the mobile telephone system.

5. A method according to claim 4, when the system is a GSM system, **characterized in** that the authentication of the GSM system is carried out using an algorithm for calculating a SRES.

6. A method according to any of claims 1 - 5, **characterized in** that the card only challenges the system, i.e. sends a random number to the system, every N time, N being a positive integer > 1, that the system challenges the card.

7. A removable memory card arranged to receive and issue information from and towards a system having means for authenticating the removable memory card, **characterized by**
- means for issuing a random number towards the system, and

- means for authenticating the system if a number returned from the system the is a correct number as verified by an algorithm stored on the card, which is fed with the same random number.

8. A removable memory card according to claim 7, **characterized by**
- means for turning off the card if the returned number is incorrect.

9. A removable memory card according to claim 8, **characterized by**
- means for only turning off the card if the system returns an incorrect number N consecutive times, N being a positive integer > 1.

10. A removable memory card according to any of claims 7 - 9, when the system is a cellular radio system, in particular a GSM system, and the removable memory card is a SIM card, **characterized by**
- means for issuing an authentication of the system in conjunction with the authentication of the SIM card by the radio system.

11. A removable memory card according to claim 10, when the system is a GSM system, **characterized in** that the authentication of the GSM system is arranged to use an algorithm for calculating a SRES.

12. A removable memory card according to any of claims 7 - 11, **characterized by** means for only challenging the system, i.e. sending a random number to the system, every N time, N being a positive integer > 1, that the system challenges the card.

13. A mobile telephone comprising a removable memory card according to any of claims 7 - 12.

14. A method of authentication in a system comprising and a first unit authentication unit communicating with a second authentication unit located in an electronic device,

characterized by the steps of:
- issuing a random number from the electronic device,
- returning a number from the system to the electronic device,
and that the electronic device authenticates the system if the returned number is a correct number as verified by an algorithm stored in the second authentication unit, which is fed with the same random number.

15. A method according to claim 14, characterized in that the electronic device turns itself off if the returned number is incorrect.

16. A method according to claim 15, characterized in that the electronic device only turns itself off if the system returns an incorrect number N consecutive times, N being a positive integer > 1.

17. A method according to any of claims 14 - 16, characterized in that the electronic device only challenges the system, i.e. sends a random number to the system, every N time, N being a positive integer > 1, that the system challenges the electronic device.

18. An electronic device arranged to receive and issue information from and towards a system having means for authenticating the electronic device, characterized by
- means for issuing a random number towards the system, and
- means for authenticating the system if a number returned from the system the is a correct number as verified by an algorithm stored in an authentication unit located in the electronic device, which is fed with the same random number.

19. An electronic device according to claim 18, characterized by
- means for turning off the electronic device if the returned number is incorrect.

20. An electronic device according to claim 19, characterized by
- means for only turning off the electronic device if the system returns an incorrect number N consecutive times, N being a

positive integer > 1.

21. An electronic device according to any of claims 18 - 20, **characterized by** means for only challenging the system, i.e. sending a random number to the system, every N time, N being a positive integer > 1, that the system challenges the electronic device.

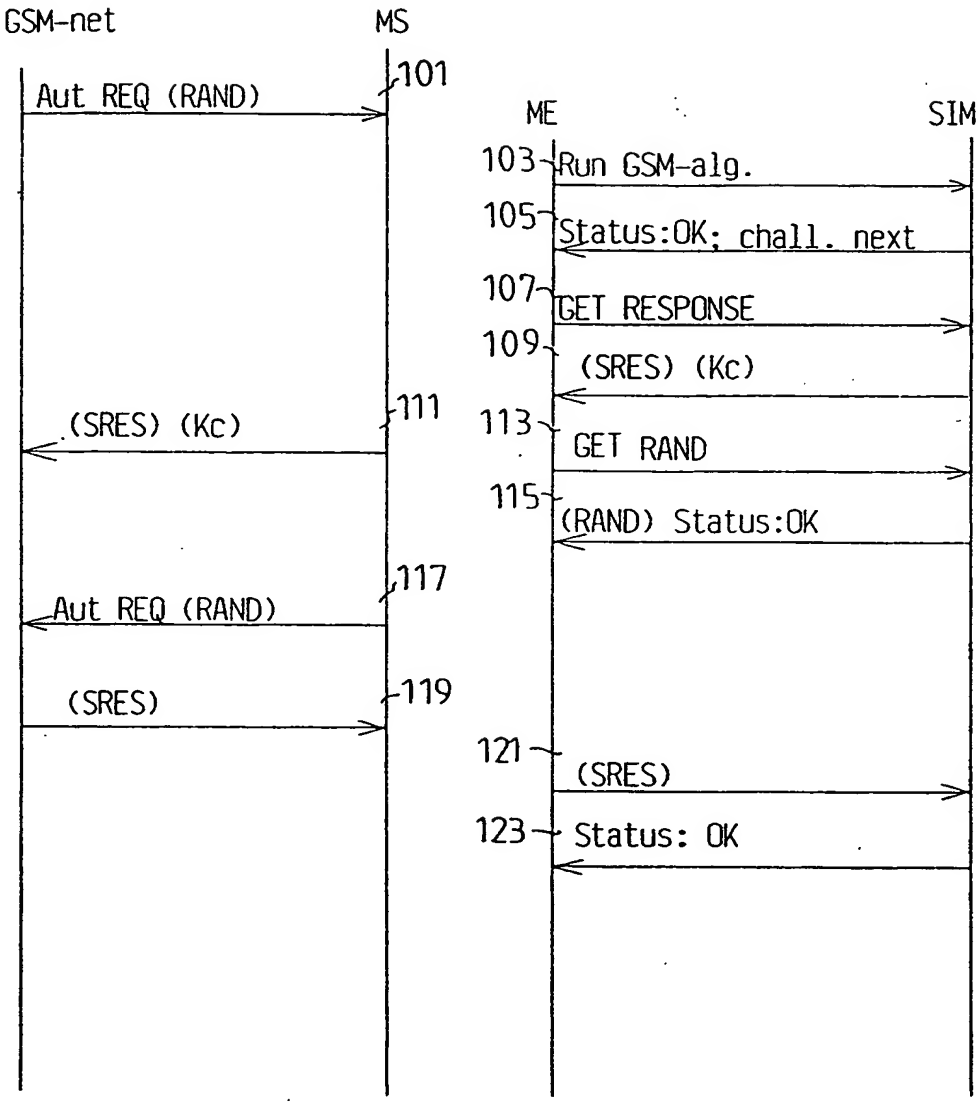


FIG. 1

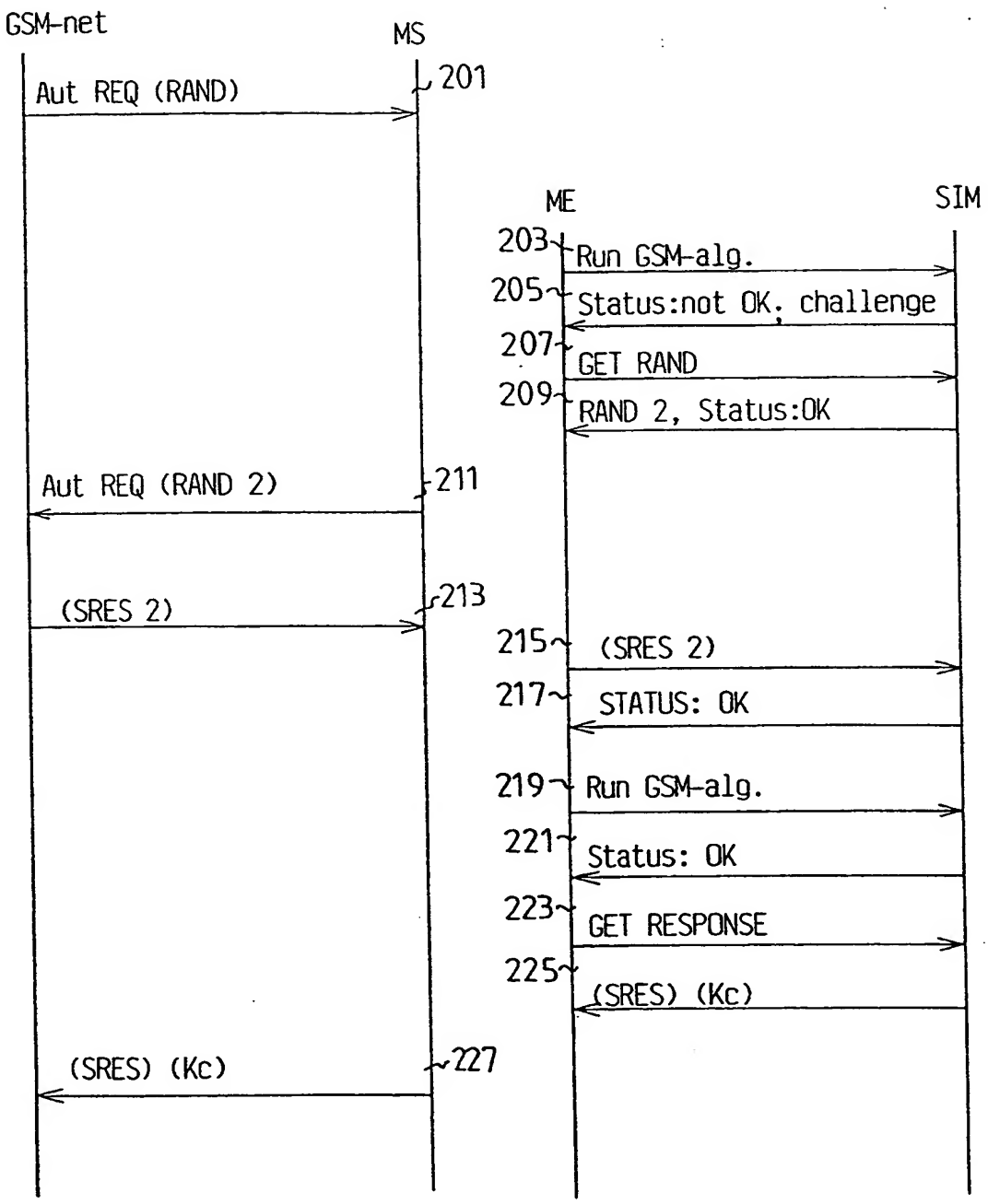


FIG.2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 99/01786

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FI 971620 A (NOKIA TELECOMMUNICATIONS OY), 17 October 1998 (17.10.98), page 7, line 10 - page 8, line 2; page 8, line 19 - line 24; page 9, line 31 - line 35, abstract --	1-21
A	EP 0651533 A2 (SUN MICROSYSTEMS, INC.), 3 May 1995 (03.05.95), abstract --	1-21
A	WO 9715161 A1 (NOKIA TELECOMMUNICATIONS OY), 24 April 1997 (24.04.97), abstract -- --------	1-21

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 March 2000	30 -03- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Stefan Hansson/cs Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/SE 99/01786

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FI 971620 A	17/10/98	AU 6733198 A	24/11/98
		WO 9849855 A	05/11/98
EP 0651533 A2	03/05/95	JP 7193569 A	28/07/95
		US 5371794 A	06/12/94
WO 9715161 A1	24/04/97	AU 7299196 A	07/05/97
		CA 2234655 A	24/04/97
		EP 0856233 A	05/08/98